Preventing Autonomous System against IP Source Address Spoofing: (PASIPS) A Novel Approach

Aman Rayamajhi[1] and Abhishek Kumar[1]
[1] NITK Surathkal/Department of Computer Engineering-Information Security, Mangalore, India
Email: {rayamajhi.aman , aksinghabsk}@gmail.com

***Abstract*— Protecting sensitive information of an Autonomous System (AS) is a critical issues. False origin with IP source address spoofing is a major threat for AS which causes serious attacks like insider attack, DDoS, unauthorized access of intellectuals and many more. Intra domain IP source address spoofing is still a challenge for security experts due to less secure router architecture and unavailability of perfect solution. In this paper, we aim to modify current LAN communication technology in private network to eliminate the possibility of any spoofed packet going outside that network. Our method is fast, light weighted, low management overhead and easy to deploy in IPv4 (preferable in IPv6), which prevent IP source address spoofing in same subnet (AS) and replay attack..**

***Index Terms*— IP spoofing; Replay Attack; DDoS Attack; Autonomous System**

I. Introduction

The Global State of Information Security 2005, a study published by PricewaterhouseCoopers and CIO, showed that 33 percent of information security attacks originated from internal employees, while 28 percent came from ex-employees and partners [20]. In many respects, insider attacks can be more difficult to detect than penetration attempts from the outside. IP address spoofing is possible because the network devices that provide connectivity between individual networks, called routers, only require inspection of the destination IP address in the packet to make routing decisions. The source IP address is not required by routers and an invalid source IP address will not affect the delivery of packets. Spoofed IP addresses are an effective way to conceal an attacker's identity during a DoS attack. However, there can be many reasons of intensions to damage the reputation of organization as well as individuals. IP source address spoofing is the easiest way to fulfill these unethical aims. IP source address spoofing waive some well known attacks like TCP SYN attack [14], Smurf attack[15], DDoS attack, conceal the real attacker, DNS amplification attack [16] etc. The obvious reason of fast increase in botnets is less secure preventive measure of IP source address spoofing. If attacker forges the IP address of another host which is situated in the same network edge or AS, it is difficult to prevent IP spoofing by many of the methods mentioned in section II. Figure 1, simplify and give clear picture of our problem statement. Attacker which belongs to network A can spoof the source IP address of other host or server within the same network. Router 1 does not have proper mechanism to verify the source IP address belongs to which host in the same network. Botnets situated in network B and C reply the all packets targeting the host or server situated in network A, cause DDoS attack. Access Control List (ACL) mechanism prevents attackers from spoofing any external addresses outside their LANs. Hence we propose to modify current communication mechanism to eliminate the possibility of any spoofed packet leaving outside the private network. Our concern is to get rid of spoofed packets generated inside private network and spoofing private addresses without involvement of existing protocols and algorithms like Kerberos [17], RADIUS [18] and IKEv2 [19] for minimum overhead. The rest of this paper includes following structure; section II introduces some important related works. The complete descriptions of our methods with different stages are described in section III. Security and performance analysis of our proposed solution is presented in section IV. Section V is the conclusion and future work.

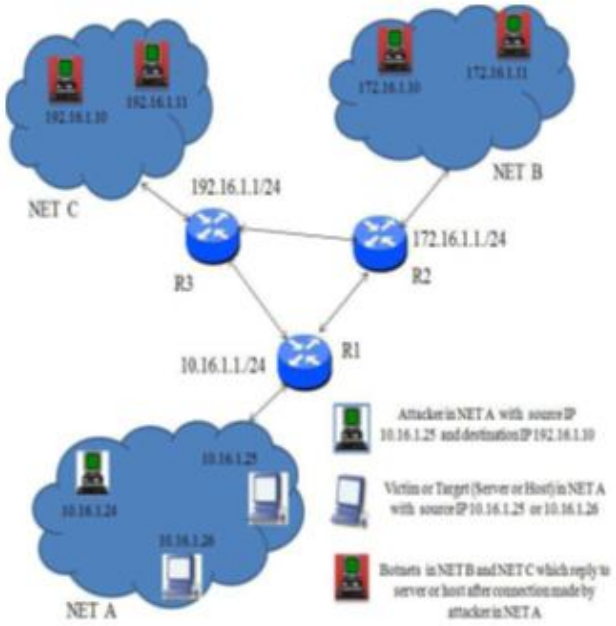

Figure 1 Attack Scenario with Attacker, Target, Victim and Botnets

II. Related Work

Many methods have been proposed and implemented to solve IP source addressing spoofing. Like SPM [1], which is based on AS to AS authentication. Methods like uRPF [2], IP traceback (SPIE [3], PPM [4], iTrace [5], APPM [6], PPPM [7] and DPM [8]), Filtering methods (Ingress [9], SAVE [11] and DPF [10]) are based on internet topology. However all of these mechanisms have some deficiencies and many of them are designed to prevent IP source addresses spoofing in inter AS level. Not much work has been focused to prevent

DOI: 01.IJNS.02.03.11

IP spoofing in same subnet (AS) due to its less concern about deployment and seriousness, which can cause a serious consequences for AS. Important work has been done in [13], which presents a signature-and-verification based IP source address spoofing prevention method, Automatic Peer-to-Peer Based Anti-Spoofing Method (APPA). The scheme proposed in [13], provide innovative approach to solve subnet IP source address spoofing, however it increases the Transaction State Machine (TSM) overhead on each host of the subnet as well as on security gateway.

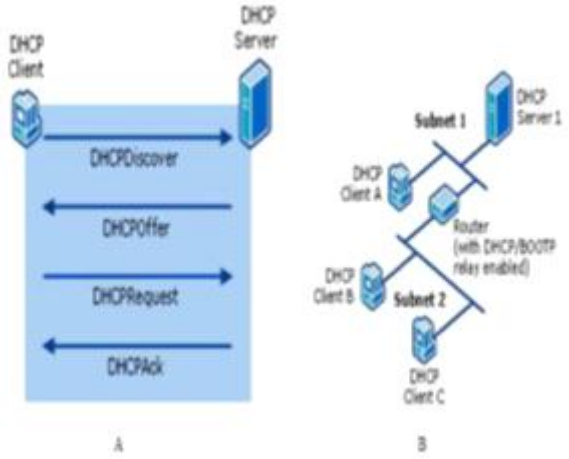

Figure 2 A. DHCP Message Flow and B. Position of Relay Enabled Router and DHCP Server

Other important work has been done in [12], in which for each time when host wants to connect internet it access security gateway for authentication and generate sessions keys involving pre-existed protocols like RADIUS [18], Kerberos [17], IKEv2 [19]. However these protocols have some drawbacks like numerous configurations, single point failure, strict time requirements (clock synchronization) etc. and it is not suitable for our problem area.

III. PROPOSED SOLUTION

Our proposed solution involves three main processes: 1. Key distribution process. 2. Fabricating packets with added signature on host. 3. Host authentication and validation process on router for each packet going outside subnet.

A. Key Distribution Process

In this process every host when boots up, gets a secret authentication key generated by relay enabled router at the time of getting IP address from DHCP server. Router keeps a mapping table where one to one mapping from set I (Set of private IP addresses assigned on subnet systems) to set K (k— k is 16 bit secret authentication key). Key distribution process involves following steps:

- Host broadcast DHCPDiscover message at boot time.
- DHCP relay enabled router respond this DHCPDiscover message generated from host and forward it to DHCP server.
- DHCP server assign particular IP from pool of addresses available for the host and forwards DHCPOffer for the same host to relay enabled router.
- Router generates 16 bit random key K and put it in DHCP option field and update the mapping table with MAC, IP and KEY records corresponding to the host. Router forwards updated DHCPOffer packet to the host.
- Host receive DHCPOffer packet hence sets it's IP and store secret key K in key cache.

B. Fabrication of Packets on Host

Host add different signature for each IP packet going outside the subnet or LAN. Each signature will be different for each IP packet generated by the host. This process strongly prevents the replay attack without generating many numbers of session's key for each IP packet. This process is a combination of two child process namely Create Signature (T, C, K) and Embed Signature (T, V). Where T is 32 bit timestamp (with hour, minutes, second and microsecond) when packet is fabricated, C is 16 bit checksum of IP header, K is 16 bit secret key of host and V is digest value.

1. **Create Signature (T, C, K)**. For each IP packet this process is called by the host to obtain the signature (T, V). Where V = Hash(C $\oplus$ K $\oplus$ T (16 bit LSB) $\oplus$ T (16 bit MSB)).
2. **Embed Signature (T, V)**. For each IP packet this process embed the 48 bit information as a pair of (T, V) in option field of IP packet as shown in Figure 3.

C. Source IP Address Validation Process

Source IP address will be validated by the relay enabled router for each IP packet going outside the AS. Router validates the source IP address by checking the host signature embedded in the IP packet. This process execute on router if and only if the checksum of the IP packet is correct to avoid the unnecessary computation on router as packet is erroneous. Router will perform following steps to validate the source IP address for each packet:

- Router retrieves the secret key K from mapping table corresponding to IP source address field of IP packet and checksum C from checksum field of IP packet.
- From option field of IP packet, 32 bit of T and 16 bit of V value extracted by the router.
- Router call Create Signature (T, C, K) process as mentioned above and calculate signature V'.
- If (T,V') == (T,V), then signature embedded into option field of IP packet will be removed so that other router in the path may not confused with the extra information in IP option field. Else, discard the packet as it is spoofed packet.

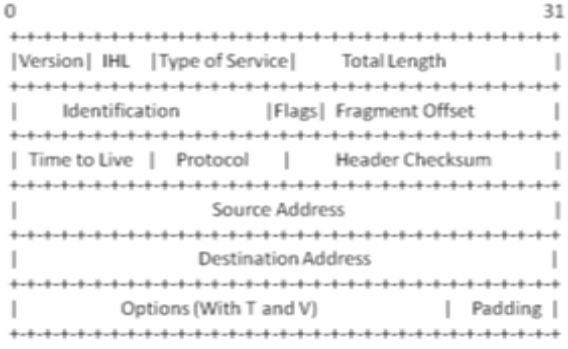

Figure 3 Fabricated IP Packet Format

DOI: 01.IJNS.02.03.11

IV. SECURITY AND PERFORMANCE ANALYSIS

In this section we analyze how secure and fast our algorithm is and other major consideration. Our algorithm uses 16 bit secret key K, 16 bit checksum C and 32 bit timestamp value. Our algorithm can use any hash algorithm (MD5, SHA1 etc.) to generate signature V which is secure enough for any AS. The hashing algorithm takes input as an XOR of K, C and T. Following statements support our algorithm's security and efficiency:

- Our algorithm get advantage of the pre-existing normal protocol for Key distribution and to send signature for validation of true IP using option field of DHCP packet and IP packet. Which utilize the packet header and reduces the unnecessary new protocol overhead.
- As host needs to store only 16 bit secret key K in key cache and router needs to store number of hosts present in subnet*32 bit (16 bit IP address + 16 bit secret key K), which is very less in memory requirement aspect for AS. Instead of storing TSM (Transaction State Machine) of 1.5Kbit for each host [13], our algorithm takes 16 bit for the same.
- Our hash algorithm generates signature of only 16 bit information, which takes very low computation time on host as well as on router. This 16 bit information is a XOR of three parameters which is very hard to guess by attacker for replay attack.
- For each IP packet the signature and timestamp will be unique. This makes confuse the attacker and secure enough in replay attack. Guessing 64 bit information by attacker will take very long time and by the time host can have different 16 bit secret key K randomly generated by router as well as different 16 bit IP address assigned by DHCP server soon after reboot the system.
- Our algorithm support incremental deployment and feasible in both IPV4 and IPV6 protocol which does not affect the normal communication protocols.

V. CONCLUSION AND FUTURE WORK

In this paper, we aim to provide solution of IP source address spoofing in same subnets. Our proposed method prevents the source address IP spoofing and it is replay attack resilient. As our algorithm have very low overhead of communication and computation, it is fast, light weighted and memory efficient as well. As we are not modifying any packet format which support the deployment of our algorithm without critics and with very low cost. However we assume that switches are not port mirror enabled. We have to keep router backup to protect against bottleneck problem. In future we provide solutions for preventing IP source address spoofing for other hierarchy of networks using our algorithm as a base, to provide fast, memory efficient and low overhead on network components

ACKNOWLEDGMENT

I would like to appreciate co-author of this paper and Department of Computer Science and Engineering-Information Security, NITK Surathkal for valuable support in this research work.

REFERENCES

[1] A.Bremler-Barr and H.Levy, "Spoofing Prevention Method", in Proceedings of IEEE INFOCOMM 2005.
[2] Cisco IDS, "Unicast reverse path forwarding", 1999.
[3] W.T.Strayer, C.EJones, F.Tchakountio, and R.R.Hain, "SPIE-IPv6: Single IPv6 Packet Traceback", IEEE Conference on Local Computer Network 2004.
[4] Savage, S., Wetherall, D., Karlin, A. and Anderson, T., Pratical network support for IP traceback, SIGCOMM 2000.
[5] Bellovin, S., ICMP Traceback messages, IETF Internet Draft draft-ietf-itrace - 03.txt 2003.
[6] Rizvi, B., Analysis of Adjusted Probabilistic Packet Marking, IPOM 2003.
[7] Al-Duwairi, B. and Manimaran, G., A Novel Packet Marking Scheme for IP Trace- back, ICPADS 2004
[8] Belenky, A. and Ansari, N., Tracing multiple attackers with deterministic packet marking (DPM),PACRIM 2003.
[9] Ferguson, P. and Senie, D., Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC2827, 2000.
[10] Park, K. and Lee, H., On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets, SIGCOMM 2001.
[11] Li, J., Mirkovic, J., Wang, M., Reiher, P., and Zhang, L., SAVE: Source Address Validity Enforcement Protocol, INFOCOM 2002.
[12] L.Z. Xie, J.Bi, J.P. Wu, "An Authentication Based Source Address Spoofing Pre vention Method Deployed in IPv6 Edge Network", Lecture Notes in Computer Science, ol. 4490, pp801-808, 2007.
[13] Yan Shen, Jun Bi, Jianping Wu, and Qiang Liu, "A Two-Level Source Address Spoofing Prevention based on Automatic Signature and Verification Mechanism",Tsinghua Science and Technology, Vol.14, No. 4, pp413-420, 2009.
[14] CERT Advisory CA-96.21. "TCP SYN flooding and IP spoofing", 2000, http://www.cert.org/advisories/CA- 621. html
[15] CERT Advisory CA-98.01. "Smurf IP denial-of-service attacks", 1998, http://www.cert.org/advisories/CA-98- Ol.html
[16] SSAC Advisory SAC008, "DNS Distributed Denial of Service (DDOS) Attacks", 2006.
[17] Kohl, J., and Neuman, C., The Kerberos Network Authentication Service (V5), RFC 1510, September 1993.
[18] Rigney, C., Willens, S., Rubens, A. and Simpson, W.: Remote Authentication Dial In User Service (RADIUS), RFC2865, 2000.
[19] Kaufman, C., Internet Key Exchange (IKEv2) Protocol, RFC 4306, 2005.
[20] Stopping insider attacks: how organizations can protect their sensitive information, IBM security and privacy 2006, http://www-935.ibm.com/services/hk/cio/pdf/.

DOI: 01.IJNS.02.03.11